



Introduction

The Department of Homeland Security (DHS) is responsible for protecting our Nation's critical infrastructure and key resources (CIKR) from physical and cyber threats. As the private and public sectors have shifted operations to internet based communications technology, all elements of the Nation's critical infrastructure have grown increasingly connected and interdependent on one-another. This demands a comprehensive approach toward continuity planning that incorporates cybersecurity. Consequently, Federal, State, territorial, tribal, and local government jurisdictions and private sector organizations must become aware of the importance of including cybersecurity considerations into continuity planning and be proactive in identifying solutions or alternative actions to challenges, gaps, or vulnerabilities in their organization's continuity plans and procedures.

Federal Initiatives

Incidents that exploit key interdependencies will require a response coordinated across all levels of government and the private sector. A comprehensive program to develop a coordinated response began with the *National Strategy to Secure Cyberspace* ("the Strategy") issued by President Bush in February 2003. In 2008, the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 established the *Comprehensive National Cybersecurity Initiative* (CNCI). The CNCI formalizes a series of continuous efforts to further safeguard our federal government systems from cyber risks and attacks. President Obama ordered a 60-day review of Federal government cybersecurity initiatives in 2009 to develop a robust strategy as to how risk is managed now and in the future. This review resulted in findings that were incorporated into the creation of the *National Cyber Incident Response Plan* in 2010. The *National Cyber Incident Response Plan* (NCIRP), currently in draft version, provides a strategic approach for integrating Federal, State, local, and tribal governments, the private sector and international partners' response to cyber incidents. The NCIRP will delineate the roles and responsibilities in dealing with a major cyber incident and will update the Cyber Incident Annex to the National Response Framework. This plan is being developed in close collaboration with partners across the Federal and State governments and industry.

"The challenges facing our nation are urgent, they involve international security—they involve our national security, both from a physical infrastructure standpoint and from an intellectual property standpoint. They involve every level from large federal institutions to large corporate institutions down to each individual who gets online—which of course is why this is something that we all need to focus upon jointly."

— Secretary Janet Napolitano,
RSA Convention, March 4, 2010

DHS National Cyber Security Division

The cyber infrastructure provides both government and the private sector with an efficient and timely means of delivering essential services around the world. In order to better protect our network systems from cyber attacks, DHS stood up the National Cyber Security Division (NCSD) in 2003. Since then, NCSD has partnered with government, industry, and academia as well as the international community to make cybersecurity a national priority and reinforce it is a shared responsibility as well as assist in implementing the *National Strategy to Secure Cyberspace* issued by President Bush in February 2003 and Homeland Security Presidential Directive 7 (HSPD-7).

The mission of NCSD is to explore and develop cybersecurity strategies to protect the Nation's critical cyber infrastructure 24 hours a day, 7 days a week. The goal of cybersecurity is the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure the information's confidentiality, integrity, and availability. In support of its mission, NCSD provides the following services to the Nation:

- Partners with all levels of government, academia, the private sector and the international community;
- Works to make cybersecurity a national priority;
- Reinforces cybersecurity is a shared responsibility;
- Works collaboratively with its stakeholders to secure cyberspace and America's cyber assets; and
- Provides a comprehensive approach to reduce and manage cyber risk.



NCSD builds and maintains an effective national cyber response system and implements a cyber-risk management program to protect critical infrastructure. Several examples of programs implemented to improve technical resiliency are:

- The United States Computer Emergency Readiness Team (US-CERT) provides response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, as well as industry and international partners.
- The EINSTEIN system, a computer network intrusion detection system (IDS), monitors government networks to identify and respond to cyber threats and attacks, improve network security, increase the resiliency of critical e-government services, and enhance the survivability of the Internet.
- The Trusted Internet Connection (TIC) Program improves the Federal by reducing external connections and providing centralized gateway monitoring.
- The Federal Information Systems Security (FISS) Information Systems Security Line of Business (ISSLoB) Program improves security of Federal information systems, reduces costs, and standardizes cybersecurity preparedness by leveraging programs such as EINSTEIN, TIC, and GSA SmartBuy.

US-CERT

Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyberattacks across the nation. US-CERT is the operational arm of NCSD at DHS and is located in the Washington DC Metropolitan area. US-CERT coordinates defense against and responses to cyberattacks across the nation. US-CERT provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. government about cybersecurity. As part of its support, the following analytical tools and programs are posted on its website (<http://www.us-cert.gov/>) for government security professionals:

- Federal Security Mailing List
- Federal Vulnerability Knowledgebase (VKB)
- US-CERT Portal
- US-CERT Einstein Program
- Internet Health and Status Service
- Security Configuration Benchmarks and Scoring Tools
- Build Security In

Additionally, US-CERT provides support for technical users and the home and casual user by posting patches, vulnerabilities, security information, and technical bulletins. There are also links for users to subscribe to email alerts and RSS feeds at <http://www.us-cert.gov/> including:

- Technical Security Alerts
- Security Bulletins
- Weekly Vulnerability Summary
- Security Alerts
- Microsoft Updates for Multiple Vulnerabilities
- Security Tips
- Understanding Your Computer: Web Browsers

Did You Know--

--An analysis of approximately 100 million compromised computers indicated that 80% of compromised machines are infected longer than a month and an unprotected computer will be compromised in less than 20 minutes!!

--Open source information provided by Trend Micro



A Brief Introduction to Cybersecurity

Risk management is the process to identify, control, and minimize the impact of natural or man-made events. Cybersecurity is one element of a comprehensive risk management program. The goal of cybersecurity is the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure the information's confidentiality, integrity, and availability. Cyber risks, vulnerabilities, and attacks on U.S. information networks can have serious consequences such as disrupting critical operations, and intellectual property, or loss of life. Preparing for, responding to, and recovering from such attacks requires the development of robust capabilities, the implementation of policies and procedures based on best practices, trained personnel, dedicated plans to mitigate risk, and ensure continuity. This also means a developed testing and exercise program is necessary to ensure all stakeholders are prepared and ready to respond when an incident occurs.

Cybersecurity issues exist across the nation and the interconnected and interdependent nature of the Internet raises risks for multiple sectors across an unlimited geographic range. Failure of or severe degradation to information technology (IT) sector or critical sector services could amplify cascading failures/stresses within various critical infrastructure. Cyber incidents could be coupled with physical attacks to disable emergency response, law enforcement capabilities, and continuity contingencies.

Moreover, cyber incidents can severely impact business/service continuity in all sectors. Cyber risks may also touch areas not traditionally associated with IT such as industrial control systems and process control systems that control everything from electric power plants to traffic signals and railroad switches. Obviously the downstream impacts of an exploitation of such a system can be extensive and spread well beyond the specific system that was originally affected.

The cyber infrastructure is subject to the same natural or man-made risks as other critical infrastructure sectors. Natural disasters can impact the cyber infrastructure through a variety of means from physical degradation to destruction. Man-made events are triggered by human actions or omissions stemming from human error, negligence, criminal behavior, and self-serving and political motives. Examples include:

- Hackers – both sophisticated and not
- Criminals
- Terrorists
- Insiders related to one of these groups (or even alone)
- Nation-state adversaries including spies
- National and/or industrial espionage

For More Information Visit:

US-CERT -- www.us-cert.gov

DHS NCSD -- http://www.dhs.gov/xabout/structure/editorial_0839.shtm

DHS National Cybersecurity Activities and Resources -- http://www.dhs.gov/files/programs/gc_1158611596104.shtm

For More Information about cyber exercises, please contact the DHS NCSD Cyber Exercise Program: CEP@dhs.gov